UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,621	04/26/2001	Harald Vater	JEK/YATER	8124

23364 7590 01/30/2009

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314-1176

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
01/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte HARALD VATER and HERMANN DREXLER

Appeal 2008-0134
Application 09/763,621
Technology Center 2100

Decided: January 30, 2009

Before HOWARD B. BLANKENSHIP, ST. JOHN COURTENAY III, and STEPHEN C. SIU, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON REQUEST FOR REHEARING

INTRODUCTION

Appellants' Request for Rehearing (filed Jul. 14, 2008) contends that we erred in our Decision on Appeal entered May 13, 2008, in which we sustained the rejection of claims 1-18.

OPINION

We hold to our previous conclusion that Appellants failed to show error in the rejection of the claims over the applied prior art. Appellants' briefs purported to show error in the rejection of the claims found by the Examiner to be anticipated by Kocher (US 2001/0053220 A1), with claim 1 being the selected claim in our review of the § 102 rejection. Appellants' Request does not show that we misapprehended or overlooked anything in making our determinations.

Appellants' arguments in the Request do not begin well, by purporting to reproduce material from page 6 of the Appeal Brief. The relevant section of the Appeal Brief does not contain any underlining, although the Request indicates that it does.

In any event, Appellants argued in the briefs that Kocher fails to disclose an operation (h) that is disguised before its execution to obtain a disguised operation (h_{KI}) that is "a different operation than" the operation (h), as recited in claim 1. Appellants submitted that Kocher teaches only "standard" Data Encryption Standard (DES) operations, not a "disguised" version of the standard algorithm. (Decision 3.) We were not persuaded of error in the rejection of claim 1, in part, because we were not persuaded that the "leak-minimizing" DES implementation described by Kocher was a "standard" DES operation. (*Id.* at 4.)

Appellants now admit that Kocher describes modifying the DES algorithm (Req. for Reh'g 2 and 4). The reference is thus not limited to describing a "standard" DES operation, as we indicated in our Decision (at

4). Appellants suggest that we were misled by Appellants' reference to Kocher's algorithm as a "standard" DES algorithm. (Req. for Reh'g 3.)

Appellants now submit that the "disguised" operation that is claimed was intended to have a different meaning from the "modified" operation described by the reference. (Req. for Reh'g 3-4.) Appellants do not, however, point to any limiting definition for "disguised" in the Specification that would distinguish over the operation described by Kocher. More important, Appellants do not point to anywhere in the briefs, that we considered in making our determinations, that relied on any limiting definition in the Specification. Nor do Appellants point to where the briefs might have referred to evidence tending to show some understanding known to the ordinary artisan that an algorithm that is "modified" to contribute against external monitoring attacks (Kocher) cannot be considered a "disguising" operation (as claimed).

Instant claim 1 recites that the "disguised operation (h_{RI}) is executed with disguised input data . . . ." Appellants admit (Req. for Reh'g 4) that Kocher disguises input data, using the same operation as described by Appellants.

Appellants argue, however, that in Appellants' system "h_{R1}(disguised input data) = y = h(x)." (Req. for Reh'g 1-2.) Unfortunately, Appellants do not tell us where this equality is set forth in instant claim 1. We do not find it in claim 1, or in any of the claims that Appellants submitted in the Claims Appendix of the Appeal Brief.

Appellants' interpretation of the equality that does not appear in claim 1 seems to be that performing the "different" operation on the disguised

input data has the same effect as performing the original operation on the undisguised input data. (*See* Req. for Reh'g 1.) Appellants' argument thus appears to rely on the third clause in the body of claim 1, reciting that the execution of the "disguised" operation "yields output data *(y)* identical with the output data *(y)* determined upon execution of the operation *(h)* with input data *(x)* . . . ."

However, as we noted in our Decision (at 4), the Examiner referred to paragraph [0036] of Kocher, which indicates that at the end of the operations, the two parts of the cyphertext "may be recombined to form the same encrypted/decrypted quantity that would have been produced by a standard DES protocol." We also took into consideration the Examiner's reliance on paragraphs [0011] ("The ciphertext is produced in permuted, blinded form, which may be easily converted to the standard DES ciphertext") and [0065] ("If the result is non-secret (e.g., cyphertext), the standard DES ciphertext is produced . . . .").

We considered, and presently consider, the reference to provide more than adequate support for the Examiner's finding that the limitations of claim 1 are met by Kocher, and Appellants' arguments do not persuade us otherwise. In the multiple pages of arguments submitted in the Request, Appellants seem to studiously avoid the description in Kocher's paragraphs [0011], [0036], and [0065]. The only remarks in the Appeal Brief that might address the Examiner's reliance on the relevant paragraphs appear to be that paragraphs [0065] and [0036] do not teach disguising of the DES operation. (*See* App. Br. 8 and 10.) We are not persuaded that Kocher fails to describe "disguising" of an operation within the meaning of claim 1. Further,

Appellants' remarks in the Appeal Brief, Reply Brief, and Request for Rehearing do not show error in the Examiner's position that Kocher describes "output data" that is within the scope of claim 1.

Appellants also allege in the Request that Kocher has a different goal than Appellants, and seem to allege that the reference does not teach the same "randomizing" operation taught by Appellants. While we can assume both allegations to be true, we remind Appellants that the rejection is for anticipation under § 102. The law of anticipation does not require that a reference "teach" what an applicant's disclosure teaches. Assuming that a reference is properly "prior art," it is only necessary that the claims "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 772 (Fed. Cir. 1983).

Moreover, most of Appellants' remarks in the Request that concern supposed differences between Appellants' invention and Kocher seem to be more particular than the apparent scope of claim 1. Appellants have not shown where the claim requires the particulars that are alleged to distinguish the invention over Kocher. The *claims* measure the invention. *See SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). Our reviewing court has repeatedly warned against confining the claims to specific embodiments described in the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc). During prosecution before the USPTO, claims are to be given their broadest reasonable interpretation, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997); *In re*

Zletz, 893 F.2d 319, 321 (Fed. Cir. 1989); *In re Prater*, 415 F.2d 1393, 1404-05 (CCPA 1969). "An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed, as much as possible, during the administrative process." *In re Zletz*, 893 F.2d at 322.

CONCLUSION

In summary, we have granted Appellants' request for rehearing to the extent that we have reconsidered our decision sustaining the rejection of claims 1-18, but we decline to modify the decision in any way.

DENIED

msc

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA VA 22314